

CLAIMS

1 1. Method for protecting the processing of sensitive information in a security
2 module with a monolithic structure, the module comprising information processing
3 means (31) and means for storing (32,33) information capable of being processed by said
4 processing means, characterized in that it comprises the following steps:

- 5 - selecting a piece of sensitive information in the storage means;
6 - determining a specific condition for the integrity of said information;
7 - reading the information and transmitting it to the processing means;
8 - verifying during the processing of the information that the specific condition is
9 satisfied;
10 - disabling the processing of the information if the specific condition is not
11 satisfied.

1 2. Method according to claim 1, wherein the information is an operation code
2 read in the storage means (32, 33), all of the operation codes being contained in a table
3 having a content determined during the manufacture of the security module, and the
4 specific integrity condition is the fact that the value of the information is equal to one of
5 several set values.

1 3. Method according to claim 2, wherein the operation code to be processed
2 is coded in the form of data bits and said bits do not all have the same binary value.

1 4. Method according to claim 1, wherein the specific integrity condition
2 consists of checking a calculated piece of integrity data using the information read in the
3 storage means (32, 33), the integrity data being calculated during the reading of the
4 information and being transmitted to the processing means, the processing means
5 calculating another piece of integrity data from the information received and checking for
6 equality between the two integrity data.

